New Challenges in Critical Infrastructures: A US Perspective

Erwann Michel-Kerjan

ECOLE POLYTECHNIQUE

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

New Challenges in Critical Infrastructures: A US Perspective

Erwann Michel-Kerjan

Avril 2003

Cahier n° 2003-004

LABORATOIRE D'ECONOMETRIE

1rue Descartes F-75005 Paris

(33) 1 55558215

http://ceco.polytechnique.fr/

mailto:labecox@poly.polytechnique.fr

New Challenges in Critical Infrastructures: A US Perspective [1]

Erwann Michel-Kerjan [2]

Avril 2003

Cahier n° 2003-004

Résumé: L'émergence d'un plus large spectre de vulnérabilités (terrorisme, sabotage, conflits locaux et catastrophes naturelles) et l'interdépendance croissante de l'activité économique rendent particulièrement vulnérables les grands réseaux vitaux des pays industrialisés. Pour y faire face, des actions importantes doivent être menées à une échelle nationale, en particulier par le développement de partenariats étroits entre le secteur public et la sphère privée.
Cet article analyse l'initiative présidentielle lancée dès 1996 aux Etats-Unis -premier pays au monde à inscrire ces questions à l'agenda du plus haut niveau décisionnel- ainsi que la structure nationale de partenariats mis en place depuis lors. Une telle démarche pourrait constituer un point de départ pour d'autres pays désireux d'élaborer leur propre analyse de vulnérabilités et leur stratégie d'amélioration.
Les événements du 11 septembre 2001, comme les attaques à l'anthrax, ont néanmoins montré que les avancées américaines ne constituaient qu'une première étape d'un processus plus global de préparation nationale; les infrastructures critiques des Etats-Unis demeurent hautement vulnérables. Enfin, plusieurs idées fausses, par trop souvent récurrentes, doivent être dépassées pour traiter beaucoup plus efficacement ces risques à grande échelle sur un plan international.

Abstract: The emergence of a larger threat spectrum -terrorism, sabotage, local conflicts, political unrest, and natural disasters- combined with the growing globalization of economic activities, makes networks highly vulnerable. Rethinking national vulnerabilities requires the creation and the improvement of long-term public-private partnerships.
The article discusses the US Presidential initiative launched in 1996 -the first initiative worldwide to put these issues on the top-level agenda- as well as the national structure of developed partnerships. It might constitute a starting point for other countries to develop their own national strategy, adapting it of course to their own national particularities.
Terrorists attacks in 2001 show, however, that such an initiative constitutes nothing but a first step in a general process to build preparedness nationwide; America still remains highly vulnerable. I conclude with a few myths that must be confronted to deal more efficiently with these new large-scale risks at an international level.

Mots clés : Risques à grande échelle - nouvelles vulnérabilites - sécurité nationale - infrastructures critiques - préparation collective - partenariats public-privés

Key Words : Large-scale risks - new vulnerabilities - national security - critical infrastructures - collective preparedness - public-private partnerships

Classification JEL: H11, H70, L90, M2

---

[1] A paraître dans the Journal of Contingencies and Crisis Management

[2] The Wharton School, Center for Risk Management, Jon Huntsman Hall, Suite 500, 3730 Walnut Street, Philadelphia, PA 19104, United States and Ecole polytechnique, Laboratoire d'économétrie, 1 rue Descartes, 75005 Paris, France. Emails: erwannmk@Wharton.upenn.edu / erwannmk@poly.polytechnique.fr

Introduction

"On October 22nd the center staff began debating *[...]* was the postal system itself contaminated? Should it be down?" (Lipton and Johnson, 2001). Crisis at the federal Center for Disease Control (CDC). Shutting down a large-scale network such as the US Postal Service, the officials knew, would inflict debilitating impacts on the economic and social continuity of the country as well as increase stress on the already sensitive psyche of the nation under siege.

Several weeks before, 9/11 terrorists made use of some elements (aircraft) of another critical network –commercial aviation– and questions were similar: How many aircraft have been hijacked? Is large part of the US airline network under the attacker's control? And the ultimate alternatives for authorities were the same: Should the closing of the entire US airspace to all flights be ordered? To stop all the aircraft that could have been hijacked, Federal Aviation Administration shut down airspace over United States to commercial traffic minutes after the two commercial jets slam into World Trade Center, first time government had taken such drastic step. As stopping the postal service would not allow avoiding future contamination if the whole system was already contaminated –one day, it would have been necessary to reopen it– the network was not closed. And 2001 events were likely to raise fundamental challenges for the security of national infrastructures[1] not only in the US, but also at the international level. A simple but crucial question emerges: How can we improve collective preparedness?

The present contribution to the JCCM special issue aims to suggest some ways of possible collective awareness to face emerging crisis situations due to large-scale breakdown or disruption of the critical infrastructures of a country. Developing partnerships between the public sector and the industry at a high decisional level is a key to adapt the organizations' readiness to new sources as well as new scales of possible disruption. In 1996, a first initiative was taken in the US to deal with those emerging large-scale risks. President Clinton launched a national study, which involved both the government (federal executives, state and local authorities) and private industry, to better understand the vulnerabilities of elements of the US infrastructure and key assets that could be critical to the business and social continuity of the

[1] For a deep analysis of the impact of anthrax crisis on long-term strategic aspects of the USPS's operation, see Reisner (2002).

country. The *President's Commission on Critical Infrastructure Protection* initiative remains unique worldwide as a preventive presidential involvement.

Most European and Asian countries still have paid little attention to those questions at a national level. In light of the 2001 attacks and under current pressure due to the high degree of uncertainty on the international scene, the US initiative may constitute, at least partially, a framework to build up collective intelligence and initiatives to better assess the vulnerabilities of interdependent critical networks and managing them (Michel-Kerjan, 2003).

This paper proceeds as follows. After the presentation of some characteristics of emerging threats, the emphasis is put on the necessity to officially clarify the true level of the stakes imposed by global issues of critical infrastructure security. Rethinking the vulnerabilities of interconnected networks, I present the national objectives of the preparedness program launched under the recommendations of the US Presidential Commission on Critical Infrastructure Protection. The outlines of this program, based upon an extended collaboration between the public and the private sectors, are then presented. Who are the key actors? What are their roles? What is their degree of interconnectivity?
As 2001 terrorist attacks dramatically showed, such an initiative constitutes, however, nothing but a first step in a general process to build preparedness at a national level; America still remains vulnerable. I conclude with a few myths we need to confront if we want to efficiently improve our capacity to deal with those new large-scale risks at an international level[2].

Emerging threats

All terrorist attacks reach a similar goal: creating fear in the targeted country. Terrorism is of course not a new risk, but the scale as well as the configuration of those attacks was rather different than more traditional terrorist attacks such as car or luggage bombing (Vareilles, 2001). What do the 9/11 events and the anthrax mailings have in common? The 2001 attacks were not physically directed against specific elements of the infrastructure. By using only four contaminated letters, attackers took great advantage of the vast capacity of the complex network of the US Postal Service[3]. The new aspect is that the

[2] Let's be absolutely clear. The purpose here is to offer a general picture –at a given time– of the initiatives launched in the US before 2001. The created partnerships are of course still evolving. And above all, those questions may evolve very quickly in the short run.
[3] For more details regarding the management of anthrax episodes by the USPS, see the contribution by Thomas Day in this special issue; Day (2003).

network itself served as a tool to diffuse and build a larger scale of threats: every envelop could have been considered as being contaminated, a potential weapon. One of the most useful and common services was becoming a source of dread about biological attacks; everyone was becoming a potential target. That configuration could have been considered only specific to the postal services. Unfortunately, even a short analysis of the dramatic September 11, 2001 events shows that the method used by terrorists is comparable in a sense that they used few elements (aircraft) of a huge network (civil aviation). As a result, all aircraft were potentially at risk.

It is one of the key lessons of those crises, which translate to a new dimension of potential destabilizations within industries operating those networks. New large-scale vulnerabilities do emerge: our critical networks can be used and reversed against ourselves as weapons for diffusing attacks and alerts throughout a country, all the elements of the network becoming potentially at risk.

At least three characteristics of those new large-scale risks stand out.

A first one is the *asymmetric value* of the attack: a small-scale but carefully targeted attack can cause large-scale reactions because of strong network interdependencies and possible cascading fallout. For instance, introducing a pathogenic agent into a nationwide distribution network may require small financial investments from attackers compared with the resulting national impact of such an action on the health and business continuity of a country. On 9/11, the terrorists did not use advanced technology to attack the US. By using only box cutters, they hijacked commercial aircraft and crashed them into civilian and government targets.

A second characteristic is the existence of an *evolving uncertainty*: terrorists can purposefully adopt their strategy of attacks based on their information on vulnerabilities of the systems and choose more vulnerable targets with respect to such information (Michel-Kerjan, 2002). The fact that attackers can choose numerous different targets implies that a huge number of potential targets need to be protected, which requires significant amount of money. Uncertainty as to targets as well as the tools that could be used to attack makes the security task very difficult to manage. Ambiguity is a complex component for decision-making.

Third, there is a *global interdependence* among similar infrastructures worldwide. No country is an island entire to itself; each national network can also be part of a global international network. For instance, the anthrax threats not only destabilized the USPS but also the whole postal activity in a lot of countries. The globalization of activities is growing. Combined with the emergence of a larger threat spectrum –terrorism, sabotage, local conflicts, political unrest, and natural disasters– that trend makes critical networks highly vulnerable not only to

direct attacks but also to cascading consequences of attacks against another similar infrastructure abroad. Thus, single events will be able to generate very quickly debilitating impacts on a whole country and, by networks' interdependence, will trigger major economic and social destabilization internationally[4].

This kind of crisis has little to do with well-known local major events such as local industrial accidents or floods. Here, the stake is to manage large-scale risks using large-scale sets of critical infrastructure being capable of inflicting significant consequences to a whole country. That requires a national and even international level of answers based upon development of public-private partnerships to deal with those emerging risks.

Putting the "Critical Infrastructures" issue on the agenda

The first initiative worldwide to seriously consider at a national level the question of critical infrastructure security has been launched by the United States. It was five years before the 9/11 events and the anthrax attacks. In 1996, President Clinton established the *President's Commission on Critical Infrastructure Protection*. Its goals were, precisely, to start dealing with those issues at the highest level. Conducting a 15-month study, the Presidential Commission studied with private sector representatives as well as academics and civil society representatives how each element of the infrastructure operates, how it might be vulnerable to breakdown or failure due to physical or cyber-attacks and what might be the cascading effect on other networks. On October 1997, The President's Commission issued its report (President's Commission, 1997). Assessing major vulnerabilities of key infrastructures of the country was a first step of an ambitious program aimed to develop collaboration between government and the private sector by creating a global architecture of partnerships on those common concerns. Such a Presidential initiative provides two clues: first, it officially clarifies the real stakes associated with the protection of large-scale critical networks; second, it put officially this question on the agenda of the highest political and decisional level; by so doing, that matter immediately became a national concern.

[4] As far as civil aviation is concerned, the 9/11 events not only impacted on the US airlines. Aviation insurers decided to cancel their third party liability policies for all airline companies in the world with only a seven-day notice, with immediate and worldwide impacts.

A new mindset: rethinking national vulnerabilities

Critical infrastructures

What are the "critical infrastructures"? The infrastructure of the United States –as one of the most of industrialized countries– is a complex system of interrelated elements. These elements have become increasingly more concentrated and more interconnected than ever. Among certain elements of the infrastructure, some are so critical that if they were destroyed or even simply disrupted, an entire region, if not the whole country, could be debilitated.

Critical infrastructures can be defined as "industries, institutions and distribution networks and systems that provide a continual flow of the goods and services essential to a country's defense and economic security and to the health, welfare and safety of its citizens" (President's Commission, 1997). Five major sectors can usually be considered critical: Critical Human Services, Information and Telecommunications, Energy, Banking and Finance as well as Physical distribution.

Some subsectors, which are themselves complex networks, provide the essential goods and services for citizens to survive. Water, food and agriculture as well as emergency services and public health are some of them. The operation of governmental services (including Defense) is also critical to administer key public functions. They are usually grouped as *Vital Human Services*. The *Information and Telecommunications* sectors along with the *Energy* (Electricity, Oil, Natural Gas) sector are also critical as most of the operation of the other networks depends on the reliable operation of those sectors. For instance, when the PanAmSat Galaxy IV communication satellite failed in May 1998, nearly 80% of the digital pagers in the US went off-line (information). Numerous credit card authorizations and ATM transactions were affected (banking), as were radio stations and broadcast transmissions (telecommunications). As doctors and other emergency services could not be paged, the country was immediately facing a crisis in emergency communication, highly critical in the healthcare system (vital human services).

The *Banking and Finance* (banks as well as financial markets) sector and *Physical distribution* (Airports, Ports, Subways, Highways, Rails, Postal services and shipping) sector also touch everyday life.

Such a categorization is obviously neither definitive nor exhaustive[5]. However, separating specific sectors helps clarifying the general picture and presents a good framework to deal with the potential vulnerabilities each of them may face[6]. A disruption of any of those networks has immediate paralyzing effects and can produce cascading fallouts over several interdependent operating networks[7].

Lack of interconnected preparedness

What did the Presidential Commission highlight in its 1997 report? Its 15-month work, which corresponded to a vulnerability recognition phase, showed numerous generic pitfalls in the US infrastructure. Two of them are particularly important for our purpose here.

First, the Commission highlighted a general underestimation of the vulnerabilities themselves. This is not surprising: in an increasingly competitive world, security (outside of conventional area of responsibility, culture, technical habits) used to be the last thing executives would be eager to spend money on. Many private sector operators considered the administrative and inspection work of regulatory and enforcement officials as making them waste of their time. Moreover, the high speed and potential ubiquity of incoming attacks were radically off cultural references: on the top-management side, there is still the idea that "you are your boss in your walls", which is actually no longer the fact when attack occurs. And the trend toward decentralization in organizational decision-making exacerbates this tendency.

Second, there was little information sharing between the government and the private sector regarding vulnerability assessment and preparedness programs. There was a lack of global warning system to alert network operators in case of an attack. It was a crucial statement as, it must be stressed, the private sector is the principal provider of goods and services and owner of 85% of the US infrastructure (Gilmore Commission, 2001). And even governmental functions strongly depend on the reliable operation of privately owned networks. Moreover, information sharing among government components (federal, state, local governments) was

[5] In this paper, the expression "critical infrastructures" has to be understood in a general sense; i.e. encompassing physical, cyber and other non-cyber-related critical infrastructures.

[6] Each of those sectors and subsectors taken separately is a very complex network. Geographical subnetworks that are also vital networks for the citizens, firms and other organizations living and operating in those areas, which depend on them in that area, compose each of them. So there is high interdependence in these elements of the infrastructure. Second, most of these networks can be greatly interdependent with each other. For instance, the finance sector needs reliable telecommunications, which needs electricity.

[7] Quite surprisingly, little academic work has been done in social sciences on the issue of risks due to national interdependency and the most fruitful contributions are just forthcoming (Kunreuther and Heal, in press; Heal and Kunreuther, 2003; Kunreuther, Heal and Orszag, 2002). Early ideas by Perrow (1984) discussed a similar issue at a local level by analyzing tight and loose coupling tendencies in several domains among which industrial accidents; on more recent concerns after 9/11 events, see Little (2002).

quite poor at that the time. And, according to the report of the Commission, the situation within companies in the private sector was quite similar (President's Commission, 1997).

National strategy: creating interconnected public-private partnerships

A National Ambition

How to deal with this situation? How to create adequate answers involving key stakeholders? Critical infrastructures are national networks. Until 1998, the missing element was, precisely, the definition and implementation of *a national strategy* to deal with those issues and coordinate actions more efficiently. The President's Commission resulted in the Presidential Decision Directive 63 (PDD 63) on May 1998 (White House, 1998). PDD 63 described a strategy for cooperative efforts by government and the private sector to protact critical infrastructures. Post 1998, and after assessing vulnerability, the second step of a global improvement process was there initiated to build a national framework for "promoting national partnerships with different roles to play between governments (federal, state, local) and infrastructures owners and operators to assess and manage new vulnerabilities from terrorism or malicious acts (physical or cyber attacks)" (PDD 63, White House, 1998). Such a global framework was recognized as essential to create a dynamic process of risk assessment and risk mitigation (increasing the potentiality that an attack on a critical infrastructure will fail as well as minimizing the disruptive impact of a successful attack).

At a federal level, responsibilities within the departments and lead agencies as sector liaisons for protecting critical infrastructures were established. An adequate answer is the creation of new structures acting as specialized interfaces at a national level: the Critical Infrastructure Assurance Office (CIAO) and the National Infrastructure Protection Center (NIPC) were created in May 1998[8].

On the industry side, first answers were also developed. The Partnership for Critical Infrastructure Security (PCIS) was established in December 1999, along with the Information Sharing and Analysis Centers (ISACs), which are specific for each critical subsector, some of which are still ongoing.

The main mission and the level of operation of those national framework's pillars depicted hereafter in Figure 1 are now presented.

[8] Hence, those new structures were established and developed before 9/11 and the subsequent changes occasioned by the creation in 2003 of the Department of Homeland Security (Homeland Security Act of 2002).

Lead agencies for sector liaisons

At the federal level, for each critical infrastructure sector, there is a single department/agency, which serves as the lead agency for liaison among the different levels of government as well as with the related industry. For instance, the Environmental Protection Agency is the lead sector liaison for water supply; the Treasury Department is the lead department for the Banking and Finance sector.

The CIAO: coordinating the federal initiatives

The mission of the Critical Infrastructure Assurance Office (CIAO) in the Department of Commerce is to identify the capabilities and responsibilities of the lead federal departments and agencies for infrastructure's continuity. Its role is also to coordinate initiatives of the federal government in critical infrastructure assurance as well as to raise national awareness about those issues. The CIAO also facilitates the partnership between the federal government, state and local governments to accomplish national assurance policy, planning and programs[9].

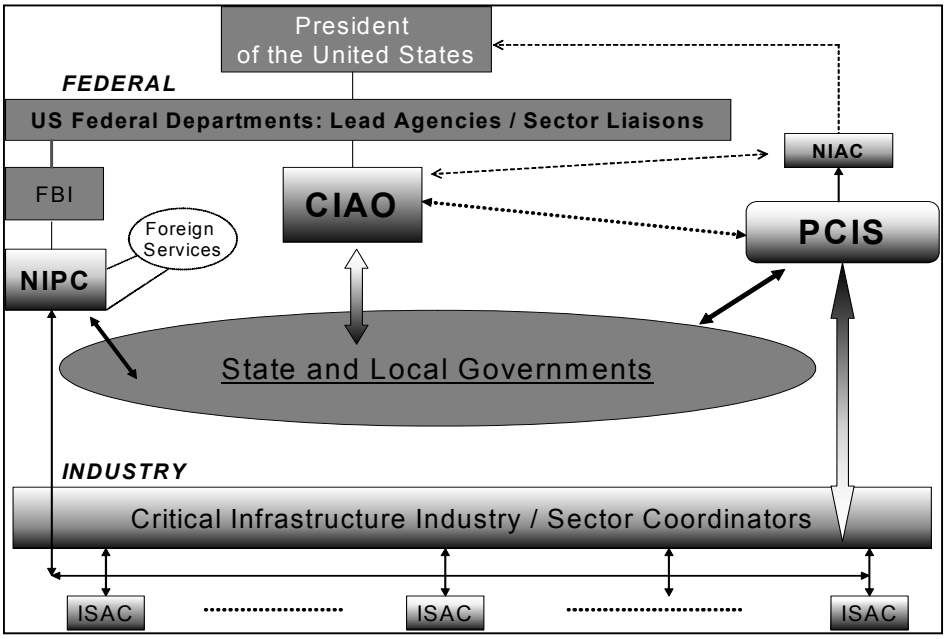

Figure 1: Public-private partnerships in US Critical Infrastructures in 2002

Finally, the CIAO is also involved in supporting the National Infrastructure Assurance Council (NIAC), a Presidential advisory committee composed of nearly 30 private sector representatives for critical infrastructure assurance policy making.

[9] The CIAO –in coordination with other federal departments and the private sector– recently elaborated the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (White House, February 2003), which provides a helpful overview of the recent efforts to assess infrastructures and key assets realized by most infrastructure sectors.

The NIPC: A Warning Center

The mission of the National Infrastructure Protection Center (NIPC) in the FBI is to provide a national focal point to gathering information on threats to critical infrastructures. It includes investigators and analysts of several agencies among which the Department of Defense, the Department of Justice, the Central Intelligence Agency, the National Security Agency, the US Secret Service and the FBI as well as the Department of Transportation, the Department of Energy or the Department of Commerce and the United States Postal Service.

It is one of the main means of facilitating and coordinating the federal governmental response to an incident as well as monitoring reconstitution efforts and mitigating attacks or investigating threats. For instance, the NIPC is linked electronically to the rest of the federal government, including other warning and operation centers, including the private sector Information Sharing and Analysis Centers (see below). The center is also reinforcing connectivity with similar centers in Australia, Canada and the UK as well as with other NIPC-like entities in foreign countries among which Japan, Israel, Germany and Sweden. Increasing the sharing of information between federal department/agencies and infrastructure owners and operators on threats, new vulnerabilities, interdependencies and ongoing attacks, and doing that both at national and international levels, the NIPC can be considered as the cornerstone of a national warning system (Figure 1).

The PCIS: a national response, from the industry

As we mentioned above, the largest part of US infrastructure is privately owned. Because of that, the private sector would be the most exposed to malicious acts against critical networks. Industry responded to the government initiatives by launching the Partnership for Critical Infrastructure Security (PCIS) in December 1999. The mission of that partnership is precisely to create and develop a cross-industry dialogue and to share experience among the private operators to improve effectiveness and efficiency of individual sector assurance efforts.

The PCIS also coordinates cross-sector initiatives launched by *sector coordinators* (analogous to the sector liaisons at the federal level) and complements public-private efforts to assure reliable provision of critical services to deal with emerging risks. It has obviously developed close relationships with CIAO for facilitating federal organizations as well as local and state-level ones to becoming effective partners of the industry. For instance, the CIAO began to

forge a broad based partnership between the industry and the government in supporting the PCIS and in launching a nation-wide outreach program targeting senior corporate leaders to make critical network assurance a matter of corporate governance and risk management[10].

Last but not least, the NIPC has also an access to the President's office through the National Infrastructure Assurance Council (NIAC)[11]. That constitutes a strong signal of the importance for the highest level of the country of the private sector's viewpoint and recommendations (Figure 1).

ISACs: warning centers for critical industries

As a result of Presidential Decision Directive 63 (White House, 1998), most of the critical infrastructures have organized themselves into Information Sharing and Analysis Centers or ISACs. An ISAC is typically an industry-led mechanism for gathering, analyzing and appropriately sanitizing and disseminating sector-specific information to their members and the NIPC.

ISACs are generally financed by their members and are designed by various sectors to meet their respective needs to acquire timely information about activities that could impact on their day-to-day operations. Hence the establishment and operation of an ISAC actually requires tremendous cooperation between its members. Because of that it also requires a well-defined preparedness model as each of the members has unique characteristics, which pose unique security challenges.

Among ISACs operating to date are the Financial services ISAC established in autumn 1999, the Telecommunication ISAC, the Electric power ISAC as well as the ones related to Information technology and e-commerce firms, Energy (oil & natural gas), Food industry, Emergency fire serves, Water supply, Surface transportation, Aviation, and the Chemical industry ISAC[12].

Scaling the answer to the problem

Through the creation of those entities and by developing awareness at different levels of operation in the government as well as in the private industry, the general architecture of the existing partnerships that have been developed since 1998 responds to a global problem –

[10] See the testimony of J. Tritak, director of the CIAO, before the US Senate; Tritak (2001).
[11] Executive Order 13231 replaces this council with the National Infrastructure Advisory Council.
[12] For a recent review of the activities of some of those ISACs, see GAO (2003).

attacks can be launched everywhere– by a high-level global framework of partnerships. Figure 1 illustrates that global configuration[13].

America the Vulnerable

With the development of such a global architecture of multi-level partnerships, the United States has been forging for the last 6 years an unprecedented effort of vulnerability recognition as well as the first significant initiatives towards more cooperation throughout federal departments and agencies, state and local governments and the private industry as well. It is, of course, only the beginning of a whole costly and long-term security improvement process. After building up a national framework –the building phase–, it may take a long time to make those partnerships fully operational. Moreover, at lower stages in these partnerships, the operational level has also to understand its role within the new national architecture. The operational phase will not be an easy task. It will require collective engagement as well as time, energy and money.

September 11, 2001 and the anthrax mailings showed the extent to which the US remained unprotected. As pointed out by a recent report by the US General Accounting Office (GAO, 2003), these facts actually reflect that a nation as large and complex as the US cannot be turned on a dime: America is still vulnerable (Flynn, 2002). In this section, I outline three problems that seem to be particularly acute for further attention. The first one –*the preparedness of local public health systems to manage biological attacks*– is currently a key topic of discussion in government administration and is largely relayed by medias. The possibilities of imminent attacks that may result from a US-led war on Iraq increase the general threats. The two other vulnerabilities –*security of the water supply system* and *security of seaports*– have been less considered until now.

Chemical and biological attacks: public health systems still unprepared

Are local public health responders and emergency services prepared to deal with biological or chemical attacks? That question is important, as those responders are the front line for ensuring the public's health and safety in case of an attack and also because response to anthrax mailings was not really reassuring on that point. The initial identification of the nature of attacks has actually been really difficult. In particular, while detecting a chemical

[13] The recent creation of the Department of Homeland Security, into which both the CIAO and NIPC are now transferred, also constitutes an important development from a government's vantage point (White House, 2003).

attack is generally not a problem, detecting a bioattack may be really problematic. Moreover, the poor capacity of authorities in autumn 2001 to organize and coordinate themselves even after anthrax was identified shows the lack of preparedness to deal with those emerging risks involving weapons of mass destruction (WMD)[14]. While one generally assumes that healthcare systems are adequately prepared for terrorism incidents, the reality strongly differs (Barbera, Macintyre, and DeAtley, 2001; Graham, 2002). National preparation could be a very long and costly process[15].

The multicountry outbreak of atypical pneumonia referred to as severe acute respiratory syndrome (SARS) might be quite illustrative on that point, as it still remains unexplained. It also showed the potential ubiquity of such phenomena made possible by commercial aviation network. At the beginning of April 2003, nearly 2,500 suspected and/or probable SARS cases – including 89 deaths – have been reported to the World Health Organization (WHO) from 18 countries around the world (WHO, 2003). That crisis also raised the question of preparedness, as it was the first time in the agency's 55-year history that it has issued a global alert against travel to a specific region or country because of an infectious disease.

Water systems

The water supply is not an infrastructure of interdependent networks over the country: water systems are in most cases owned and operated by local water companies as well as maintained by local authorities. That local level's involvement in security differs highly from one region to another and is usually slow in adopting new safety technology. Most of those water systems have still not implemented any testing and monitoring capacity of public water supplies for pathogenic contaminants. Even locally, the contamination of such a system would

[14] Two years ago, the RAND conducted a nation-wide study to measure the degree of preparedness of local health and emerging services to chemical and biological attacks. Such a study is interesting as it offers a broad overview through two measures: (1) whether the respondent organizations have a plan to address the particular incident and (2) among those with plan, whether the plan has been exercised in the last two years. The studied scenario was not a large-scale attack but a moderately size chemical/biological one (200 injuries). Based on the survey results, plans and exercises are more common for chemical incidents than for biological ones but remain small in both cases. More problematic is the fact that for the biological incident scenario, less than 7 percent of any type of local organizations (police, fire, public health, offices of emergency management, emergency medical services, hospitals) positively answered to the two questions. Moreover, one-quarter of biological incident exercises developed by hospitals and local public health agencies did not test how they would communicate with police, fire and emergency medical services (Fricker, Jacobson and Davis, 2002).

[15] From 1996 to 1999, the Federal government provided WMD response training to 134,000 first responders, only 2 percent of whom received hands-on training with live chemical agents. Moreover, 134,000 fall short of the estimated 9 million first responders to be trained in the US (Council of Foreign Relations, 2002).

inflict thousands of injuries or even deaths that would be immediately highly publicized as the inability of authorities to provide safely citizens with the basic element of life.

Seaports

As I pointed out earlier in the discussion, on 9/11, the terrorists did not use sophisticated weapons but box cutters and obliged federal authorities to order the closing of US airspace to all flights. Using a few contaminated envelopes, attackers obliged to seriously consider the possibility to temporary close the whole postal network in the US. It is obvious that if an attack –whatever the source– were to happen next month involving the sea transportation network, the alternative would be likely the same: does the closing of all the ports around the nation have to be ordered? Does the transportation system carrying millions of tons of trade per day to the country have to be stopped?

As mentioned in a recent report by the Council of Foreign Relations, a closure of US ports for several weeks would impact on the whole industry. If an attack uses a container, as letter or aircraft have been used, it would raise concern about the 20,000 containers arriving in US ports every day as well as the whole container traffic worldwide. For instance, megaports such as Singapore and Rotterdam would have to close some of their gates to prevent containers piling up on their limited pier space (Flynn, 2002). As a result of a *global interdependence*, global commerce would be in danger. As of today, such a question still often gets left out of discussions regarding US critical infrastructure security (Council of Foreign Relations, 2002).

Getting over with myths

On a more general level it is worth noting three recurrent views that strongly limit the development of collective initiatives to deal efficiently with emerging vulnerabilities in critical infrastructures. They are some key issues all countries will have to seriously consider and put as soon as possible on the agenda of the highest executive levels in order to be prepared to manage emerging large-scale risks.

Myth 1. Only the US is vulnerable

9/11 events and anthrax mailings occurred in the US. However, had those events occurred in another industrialized country, the crisis would have been the same or even worse

as those issues have not yet been integrated in a national strategy abroad. Every country is, however, highly dependent on the reliable operation of its critical networks. Even if the US is often cited in the medias as the first target for terrorists, no country should underestimate the vulnerability of its critical infrastructure. There are at least three reasons for that. First, according to experts on terrorism, European countries also face a dangerous expansion of terrorist groups in recent years (Assemblée Nationale, 2002). Second, threats do not come only from terrorism. Malicious acts, which may have nothing to do with terrorism, would inflict the same debilitating impact on a nation or a group of nations by paralyzing critical networks. Third, even if this contribution focuses on emerging vulnerabilities, more traditional sources of catastrophic risks remain, such as natural disasters and technological failures. They are not specific to the US. For instance, storms in France in December 1999 as well as ice storm in Canada in January 1998 destroyed the largest part of the electricity network of those countries, reminding the major collapse of all the Kobe infrastructures after the 1995 earthquake.

Myth 2. Managing new vulnerabilities does not require preparedness

Members of the government as well as most CEOs and top-level executives may have to face unpleasant and unexpected unknown situations due to the potential breakdown of critical infrastructures in the short term. A recent survey realized by the Council of Competitiveness in 2002–a Washington, DC-based group of CEOs, university presidents and labor unions leaders– found that only 70% of senior executives said they were concerned about a terrorist attack to their business. Half of those had done anything about it[16].

New types of crisis, however, are going to inflict irreversible consequences to the involved organizations, and that faster than ever. Being too optimistic by simply pretending that preparedness is unnecessary is clearly not a viable long-term strategy[17]. Hence, it must be well understood that preparation and collective work on large-scale emerging risks may constitute the unique framework to do a better job in crisis time (Gilbert, 2002; Guilhou and Lagadec, 2002). Such an anticipative work would even open the door to success as being a clear competitive advantage. The cost of preparation falls short of the significant consequences of emerging risks[18]. And terrorists could learn and adapt their strategies more

[16] Cited in Wharton School (2003).
[17] As Norman Augustine made the point few years ago, more than 50% of CEO's have no crisis plan, but 97% are confident that they will respond well if crisis occurs (Augustine, 1995).
[18] The impact of the four 9/11 hijackings is illustrative.

rapidly than some official circles (Rosenthal, Charles, 'T Hart, 1989). When the attacks occur, time for learning is over[19].

Myth 3. Building trust is an easy task

Making critical networks safer is a task that involves not only public entities and officials, but private entities and officials as well. The need for public-private partnerships has become necessary for many reasons that are developed above. Creating and developing such partnerships, however, is not an easy task: the habits, cultures, references and attempts of the two sectors differ in numerous ways (Godard, Henry, Lagadec and Michel-Kerjan, 2002). The integration of the private sector into domestic preparedness programs may take time and create strong opposition because of historical reasons, cost concerns[20], and legal impediments as well (Kayyem and Chang, 2002). The alternative –stopping a whole activity– is, conversely, not really attractive. Above all, developing collective initiatives requires being able to trust the other stakeholders. The existence of trust would be an essential element of all enduring and successful public-private partnerships. That aspect of any partnership is a key stake as one of the most fundamental qualities of trust has been known for ages. Trust is fragile (Slovic, 1993, 1999; Seligman, 2000). Crisis episodes –perhaps more than any other situations– can destroy it very easily. The problem of Trust is not the least one.

Concluding notes: a collective responsibility

After the recognition by the White House of those issues as critical, after 5 years of vulnerability assessment and creation of multi-level partnerships to mitigate the risk in the United States, the 9/11 terrorists attacks as well as the anthrax mailings revealed cascading impacts due to strong critical infrastructure sector interdependencies, which still often get left out of analyses regarding US critical infrastructure security (Gordon, 2003; GAO, 2003). Those events also revealed that the route would be nothing but a very long, complex and costly one.

[19] Recent research on anticipation versus improvisation as sources of organization resilience while experiencing an unexpected situation can be fruitful to consider; see for instance Rerup (2001), Hatch (1997), Berliner (1994).
[20] For instance, regarding seaport security, "US-bound cargo ships preparing to leave any foreign port must now file a manifest with US customs inspectors certifying the contents of every container. The new regulation, designed to prevent bombs entering the US in containers, will adds costs, delay shipments, and may result in the shutdown of next day delivery services" (Wharton School, 2003).

The US initiative may constitute a framework for other countries to develop their own national strategy by adapting it to national particularities. Two elements appear fundamental for succeeding: proactive behavior and challenge. Proactive behavior: do not wait for a series of events before preparing the country and developing new partnerships. Challenge: those risks are nothing but large-scale risks involving whole critical networks; local answers –when they exist and are regularly and efficiently tested– will not be longer sufficient: they have to be part of a national or even international strategy of security improvement.

The *European Cooperation on Postal Security* closed meeting in Paris last autumn, which was organized in that spirit and that involved top-executives from postal services and authorities from no less than 26 countries[21], may constitute an initiative to follow.

In the end, the security of critical infrastructures is a matter of collective responsibility –collective courage I would say. With current high tensions on the international scene and as attackers have only to be lucky once, the next two years may be critical.

Acknowledgement

The article is based on the presentation made at the meeting "European Cooperation on Postal Security: From Anthrax and Beyond" in Paris, November 27-28, 2002. I thank Thomas Day, Claude Henry, Paul Kleindorfer, Howard Kunreuther, Patrick Lagadec, Olivier Oullier, Robert Reisner, Claus Rerup and Stefan Spinler for helpful discussions and comments. Preparation of this paper was supported by the joint project "Interdependent Security" between the Wharton School and Columbia University, by the Institut Vivendi Environnement and the Ecole Polytechnique in Paris.

References

Assemblée Nationale (2002), *Livre noir. Contributions à la conférence internationale du 05 février 2002 sur le thème « Terrorisme et responsabilité pénale internationale »,* Paris.

Augustine, N. (1995), "Managing the Crisis You Tried to Prevent', in N. Augustine, J. Quelch and A. Sharma (eds.), *Harvard Business Review on Crisis Management*, pp. 1-32.

Barbera, J., Macintyre, A. and DeAtley, C. (2001), "Ambulances to Nowhere: America's Critical Shortfall in Medical Preparedness for catastrophic Terrorism", *BCSIA Discussion Paper* 2001-15, John F. Kennedy School of Government, Harvard University.

[21] Among which France and the United States.

Berliner, P.F. (1994), *Thinking in Jazz: The Infinite Art of Improvisation*. Chicago University Press, Chicago.

Boin, R.A. and Lagadec, P. (2000), "Preparing for the Future: Critical Challenges in Crisis Management", *Journal of Contingencies and Crisis Management*, vol.8, No. 4, December, pp. 185-191.

Council of Foreign Relations (2002), *America-Still Unprepared, Still in Danger*. New York.

Day, T. (2003), "The Autumn 2001 Anthrax Attacks on the United States Postal Service: The Consequences and Responses", forthcoming, *Journal of Contingencies and Crisis Management.*

Executive Order 13231 (2001), Federal Register, Vol. 86, No. 202, pp. 53063-53071, October 18, 2001.

Executive Session on Domestic Preparedness. *Beyond the Beltway: Focusing on Hometown Security.* John F. Kennedy School of Government, Harvard University, September 3, 2002.

Flynn, S. (2002), "America the Vulnerable", *Foreign Affairs*, Vol. 81, No. 1, Jan./Feb.2002, pp. 60-74.

Fricker, R., Jacobson, J. and Davis, L. (2002), "Measuring and Evaluating Local Preparedness for a Chemical of Biological Terrorist Attack", *RAND Issue Paper.*

General Accounting Office (2003), *Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors*, United States General Accounting Office, Report to the Committee on Energy and Commerce, House of Representatives. February 28, 2003, Washington, DC.

Gilbert, C. (2002), "From One Crisis to the Other: The Shift of Research Interests in France", *Journal of Contingencies and Crisis Management,* Vol. 10, No. 4, pp. 192-202.

Gilmore Commission (2001), *Third Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction*, December 15, 2001.

Godard, O., Henry, C., Lagadec, P. and Michel-Kerjan, E. (2002), *Traité des nouveaux risques : Précaution, Crise, Assurance*. Gallimard, Folio actuel, Paris.

Gordon, L. (2003), "Improving Homeland Security and Critical Infrastructure Protection and Continuity Efforts", available on www.gwu.edu/~rpsol/homeland.

Graham, A. (2002), "Unprepared for Smallpox." *Washington Post* A, 26 December: 39.

Guilhou, X. and Lagadec, P. (2002), *La fin du risqué zero*, Eyrolles éditions, Paris.

Hatch, M.J. (1998), "Jazzing up the Theory of Organizational Improvisation", *Advances in Strategic Management*, 14, 181-191.

Heal, G. and Kunreuther, H. (2003), "You Only Die Once: Managing Discrete Interdependent Risks" Working paper, Columbia Business School and Wharton Risk Management and Decision Processes Center, February.

Kayyem, J. and Chang, P. (2002), "Beyond Business Continuity: The Role of the Private Sector in Preparedness Planning." *Perspectives on Preparedness*, august 2002.

Kunreuther, H. and Heal, G. (in press), "Interdependent Security", *Journal of Risk and Uncertainty*.

Kunreuther, H., Heal, H. and Orszag, P. (2002), "Interdependent Security: Implications for Homeland Security Policy and Other Areas", in *The Brookings Institution Policy Brief,* #108, October 2002.

Lipton, E. and Johnson, K. (2001), "Tracking Bioterrorism's Tangled Course", *New York Times Magazine*, December 26.

Little, R. (2002), "Controlling Cascading Failure: Understanding The Vulnerabilities of Interconnected Infrastructures", *Journal of Urban Technology*, Vol. 9, No. 1, pp. 109-123.

Michel-Kerjan. E. (2003), "Risques catastrophiques et réseaux vitaux : de nouvelles vulnérabilités", working paper, Center for Risk Management, The Wharton School*;* forthcoming in *Revue Flux – International Scientific Quarterly on Networks and Territories*.

Michel-Kerjan. E. (2002), "New Vulnerabilities in Critical Infrastructures", *Wharton Risk Management Review*, Fall 2002.

Perrow, C. (1984), *Normal Accidents*: *Living with High-Risk Technologies*, Basic Books, New York.

The President's Commission on Critical Infrastructure Protection (1997), *Critical Foundations: Protecting America's Infrastructures*, Washington D.C.

Reisner, R. (2002), "Homeland Security Brings Ratepayers vs. Taxpayers To Center Stage", in M. Crew and P. Kleindorfer (eds.), *Postal and Delivery Services. Delivering on Competition*, Kluwer Academic Publishers, pp.223-242.

Rerup, C. (2001), " 'Houston, we have a problem': Anticipation and improvisation as sources of organizational resilience", *Comportamento Organizacionale E Gestao*, vol.7 (1), pp.27-44.

Rosenthal, U., Charles, M.T. and 'T Hart, P. (Eds) (1989), *Coping with crises: The Management of Disasters, Riots and Terrorism.* Charles Thomas Publisher, Springfield, IL.

Seligman, A. (2000), *The Problem of Trust*. Princeton University Press, Princeton, NJ.

Slovic, P. (1999), "Trust, Emotion, Sex, Politics, and Science: Surveying the Risk-Assessment Battlefield." *Risk Analysis*, Vol.19, No. 4, pp.689-701.

Slovic, P. (1993), "Perceived Risk, Trust, and Democracy" *Risk Analysis*, Vol. 13, No. 6, pp.675-682.

Tritak, J. (2001), *Testimony before the US Senate, "Critical Infrastructure Protection: Who's in Charge?" Committee of Governmental Affairs*, October 4, 2001.

Vareilles, T. (2001), *Encyclopédie du terrorisme international.* Paris : Editions l'Harmattan, coll. 'culture du renseignement'.

Wharton School (2003), "How Far Should Business Go to Protect Itself Against Terrorism?", *Knowledge at Wharton, Strategic management*, February 2003.

White House (2003), *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. February 2003, Washington, D.C.

White House (2002), *Homeland Security Act of 2002*. November 25, 2002, Washington, D.C.

White House (1998), *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*. May 22, 1998, Washington, D.C.

World Health Organization (2003), "Cumulative number of Reported Cases of Severe Acute Respiratory Syndrome (SARS)", available on www.who.int as of April 4, 2003.